ProtonMail has also flip-flopped their "no logs" policy, when they were pitching on IndieGoGo they promised that the service was "fully anonymous" & that unlike Yahoo or Google that ProtonMail would never track users, would never log IP address, etc etc but now anyone who calls them out on why they did a reverse 180 on their longstanding policy gets immediately accused as a criminal.

They have also went against policy of never handing out data unless a valid court order comes through first, & now they are giving out data to agents left & right without court order etc... To make matters worse, they are closing accounts & banning accounts of PAID users merely on false allegations alone, so despite the claim that Protonmail user accounts are protected by privacy, security, a data center in a mountain, redundancy, etc all it really takes for effective denial of service is a random pissed off person on the internet to contact Protonmail staff with false allegations against a Protonmail user & then Protonmail user's account will be immediately banned without question, without investigation, without evidence & with zero due process & not even a semblance of such. Protonmail cannot be trusted to do the right thing or to make the right judgment calls. Their slogan should be something like : ***"Protonmail, where you are always at most one false allegation away from losing all your emails"***

But Proton is more than happy to take your money, making it impossible to disable autorenew, & impossible to delete your credit card info (unless you forcibly downgrade first) & once they force you to downgrade you lose all pro-rated periods that you had already paid for upfront & then you are locked in since they also disable your main email alias & disable the ability to export out via their buggy "Bridge" program, even if you had already paid upfront for the entire billing cycle! Effectively, this is unlawful "lock-in" against the GDPR laws.

https://archive.org/details/ProtonmailOutrightBanningPaidUsersFromSendingEmailsWithNoWarningProtonMail

https://www.bestvpn.co/protonvpn-is-scam/

During the IndieGoGo campaign in which Protonmail successfully gained in close to half a million dollars of donations/ crowd funded investor monies etc the promise (or at least the public pitch) was

always that it was "FULLY Anonymous" & that there was "No tracking or logging of personally identifiable information." & again wording of : " No tracking or logging of user data." & also that of "Unlike competing services, we do not save any tracking information. We do not record metadata such as the IP addresses used to log into accounts. We also have no way to scan encrypted messages to serve targeted advertisements. To protect user privacy, ProtonMail does not require any personally identifiable information to register." etc etc etc

So why did you start tracking IP addressess & logging info & what was the reason & rationale for such a dramatic departure from what you earlier claimed had "set you apart" essentially from the competing services like Google & Yahoo? If like the case of the child kidnapping was important enough for you to cooperate with law enforcement of a foreign government without first officially obtaining a valid court order then it should likewise also be important enough for you to be abundantly clear with your end-users & userbase that you do make exceptions to the things that you had essentially earlier promised that you would not infringe upon.

Formalities matter to the extent that they are/were used as a selling or pitching point of your product or service. If you had previously stated that Protonmail doesn't cooperate without first obtaining a valid court order, but then go on to make exceptions, then you are going against your own official policy. Legal process exists for a reason, policy exists for a reason, following it to the letter is important, because outside of technicial controls, if you really think about it, that's all we have left, that's all anybody ever has in truth. Protonmail should not elevate itself to the position of being the judiciary & making decisions that are required by a judge via a court order.

I don't recall exactly which post, but on reddit recently Protonmail took the stance that Protonmail is actually better than a judge when it comes down to deciding if data should be handed over or something to that effect. If you stop following the legal process & due process, stop waiting for the official court order & instead become your own quasi-judge then what else is there left to safeguard? If you directly talk to trusted "agents" & don't wait for the court order itself, then what is the point? But Protonmail should not take place of the judiciary least you give yourself powers that you don't legally have. You stated that it comes down to be about "trust", but we see so many governments & conglomerates alike (including Google) use the often trite "just trust us" excuse. History has shown that is ripe to be taken advantage of. There are technicial safeguards, & there are legal safeguards. The much promised & long overdue ability to import users own pgp keys (technicial safeguard) is no

where to be seen & now it appears the legal safeguards (official court order & nothing less will do) is losing its integrity as well...

This matter potentially is further complicated by the fact that you are promoting other services like VPN in the form of ProtonVPN in addition & conjunction to your email service. The common response to those who don't want their IP address tracked when accessing their email is just to use a VPN. But the concern is for a company that went back & regened on its policy of not tracking/logging email users ("fully anonymous") the precedent has already been set for this to happen again & there is no guarantee the same or similiar won't be effectuated for ProtonVPN as well.

At the very least, this puts Protonmail in the uncomfortable position of having to make a difficult decision in such edge cases where had the user not consolidated all his privacy services into one Proton, & used for example NordVPN when accessing Protonmail as opposed to ProtonVPN when accessing Protonmail, then this wouldn't have even been an issue in the first place. So we are talking about avoiding single points of failure, both technically (when you get DDoS often both Protonmail & ProtonVPN are down or otherwise inaccessible) as well as from a legal or political standpoint (ProtonVPN may choose in the future to start logging IP addresses or handing them over too, which would entirely defeat the point & purpose of using a VPN (in this case ProtonVPN) in order to prevent tracking/logging from Protonmail) The new revelations of ProtonVPN partnership & close ties to TesoNet does not bode well to instill confidence that ProtonVPN will not be abused in the same manner & fashion that ProtonMail has been watered down, with its privacy scaled back, & its selling points totally obliterated...

Protonmail's recent aggregation of statistics in the reports of requests was done in the name of being more efficient & expedient. imho, I think the point that is often missed is that the whole point is it is/was intended to make it difficult & not to make it easy. By changing the policy or at least the way request are being reported & by aggregating them in mass that is one step towards trivializing these requests as just another consequence of doing business & very ironically this is the exact very same justification those in power use for the deployment & implementation & usage of "Mass surveillance" in general, which if I'm not incorrect, is the whole alleged & purported point of your service is to counter that. This is not sliding in the right direction, that much is without doubt.

Proton has in recent times much more heavily pivoted towards the "just trust us" motto, at times & in many critical junctions resorting & reducing it to "its really all comes down to be about trust", & of course convinently taking the defacto stance & the 'a priori' assumption from the company is that anything Proton branded or Proton labeled is thus automatically exempt from scrutiny & almost as if capitalizing on their (imho ill-gotten & undeserved) broad publicity & substituting that in place of the earlier technicial safeguards that were promised to its users from long ago. I find this sort of unwarranted "Exceptionalism" to be toxic to the core essence of true privacy & security.. In place of the long promised & much touted but yet still to be materialized technicial safeguards (ability to export/import own pgp keys, ability to increase key strength, the promise of full open source, a standalone mail client or browser extension, etc etc etc) & the increasingly abandoning of the legal process, watering down of the product & services in terms of privacy first etc & also the sliding down of the slippery slope (giving out data prior to getting court orders, contrarly to Proton's own policy & something that was used as a selling point & product/service differentiation point when pitching to the public & trying to get user adoption & tracking) Proton merely shifts all of these to the side by pivoting towards a new paradigm of blind trust & mindless faith in all things "proton"...

The supreme ultimate irony is that by & through its actions, inactions, & the new facts of revelations, even taking the position most generous & favorable to Protonmail, one can only reasonable conclude that Protonmail is not deserving & does not merit the good faith trust that its users & the general public may have placed in this company, & its products & services. Without this trust, without technicial protections & without legal safeguards, Protonmail is nothing, infact I dare say it is worse than Gmail because it gives those most concerned about privacy the very defintion of false sense of security...